CLARK UNIVERSITY

Exercises
Math 225 Modern Algebra
Fall 2017

14. Prove the following three statements about greatest common divisors.

$\gcd(a, b + ka) = \gcd(a, b)$.
$\gcd(ak, bk) = k \gcd(a, b)$.
If $d = \gcd(a, b)$ then $\gcd(a/d, b/d) = 1$.

As usual, there are various different proofs that you might derive for these. The ones I give are representative.

Proof. To show $\gcd(a, b + ka) = \gcd(a, b)$. One general method that works to show that two greatest common divisors are the same is to show that the common divisors (greatest or not) of the first are the same as the common divisors of the second. For if all the common divisors are the same, then greatest common divisors must also be the same.

In this case, we would show $d|a$ and $d|(b+ka)$ if and only if $d|a$ and $d|b$.

$\Rightarrow$: Assume $d|a$ and $d|(b + ka)$. Then $d|ka$ (property 2 mentioned in the text, or you could show it directly), so $d|((b + ka) - ka)$ (property 5). Thus $d|b$.

$\Leftarrow$: Assume $d|a$ and $d|b$. Then $d|ka$ (property 2 again), therefore $d|(b + ka)$ (property 5 again). Q.E.D.

Proof. To show $\gcd(ak, bk) = k \gcd(a, b)$.

Let $d = \gcd(a, b)$ and $c = \gcd(ak, bk)$. We'll show that $kd = c$ by showing that both $kd|c$ and $c|kd$.

Since d divides both a and b, therefore kd divides both ak and bk. But c divides every divisor of both ka and kb, therefore c divides kd.

Since $d = \gcd(a, b)$, it is a linear combination of a and b. That is, $d = xa + yb$. So $dk = xka + ykb$ for some integers x and y. But c divides both ka and kb, so c also divides dk.

Since both $kd|c$ and $c|kd$, therefore $c = kd$. Q.E.D.

Note that not all linear combinations of a and b equal the $\gcd(a, b)$, so when showing something is equal to the gcd, it isn't enough to show it's a linear combination of a and b.

Proof. To show that $d = \gcd(a, b)$ implies $\gcd(a/d, b/d) = 1$.

Let $e = a/d$ and $f = b/d$. Then by the preceding statement $d = \gcd(a, b) = \gcd(de, df) = d \gcd(e, f)$. Therefore $1 = \gcd(e, f)$, which says $\gcd(a/d, b/d) = 1$. Q.E.D.

17–26. These are all proofs of basic theorems of fields. Each should be carefully stated with justifications for each step. Those justifications should be axioms of fields, definitions, or previously proved theorems. So, for example, you could use the results in exercise 17 in the proof of exercise 18.

There are usually several different proofs for each statement, so the ones I give below are only representative proofs, not the only possible proofs.

17. Prove that 0 is unique. That is, there is only one element x of a field that has the property that for all y, $x + y = y$. (The proof that 1 is unique is similar.)

Proof. Suppose that $x + y = y$. The axiom of additive inverses for fields says that there is an element z that is an additive inverse of y so that $y+z = 0$. Add z to each side of the given equation $x+y = y$ to conclude that $(x+y)+z = y+z$. Since $y + z = 0$, therefore $(x + y) + z = 0$. Since addition is associative in a field, therefore $x + (y + z) = 0$. Again, $y + z = 0$, so $x + 0 = 0$. By the axiom for the additive identity for fields, it follows that $x = 0$. Thus, the only element of the field that has this property is 0. Q.E.D.

Here's an alternate proof which is a little shorter: Suppose that there are two zeroes, denote them 0 and $0'$. Then since 0 is a zero of the field, therefore $0 + 0' = 0'$. But $0'$ is also a zero of the field, so $0' + 0 = 0$. Since $0 + 0'$ is equal to both $0'$ and to 0, therefore $0' = 0$. Thus, there is only one zero in a field. Q.E.D.

18. Prove that each number has only one negation. That is, for each x there is only one y such that $x + y = 0$. (The proof that reciprocals of nonzero elements are unique is similar.)

Proof. Suppose that $x + y = 0$ and that $x + y' = 0$ as well. Then $x+y = x+y'$. Let z be an additive inverse of x so that $z+x = 0$. Add z to each side of the equation $x+y = x+y'$ to conclude that $z+(x+y) = z+(x+y')$. Using associativity, we can rewrite that as $(z + x) + y = (z + x) + y'$. But $z + x = 0$, so $0 + y = 0 + y'$. Since 0 is the additive identity, therefore $y = y'$. Thus, there is only one additive inverse of an element in a field Q.E.D.

Now that we've got this theorem, we can denote the unique additive inverse of an element x as $-x$.

19. Prove that the inverses of the identity elements are themselves, that is, $-0 = 0$, and $1^{-1} = 1$.

Proof. In light of the previous exersize, in order to show that something y is the additive inverse of 0, it's enough to show that $0 + y = 0$. But $0 + 0 = 0$, therefore 0 is the additive inverse of 0, that is, $-0 = 0$.

Likewise, to show that y is the multiplicative inverse of 1, it's enough to show that $1y = 1$. But $1 \cdot 1 = 1$, so 1 is the multiplicative inverse of 1, that is $1^{-1} = 1$. Q.E.D.

20. Prove that multiplication distributes over subtraction: $x(y - z) = xy - xz$.

Proof. Subtraction is defined in terms of addition of the negation. So $x(y - z)$ means $x(y + -z)$, and $xy - xz$ means $xy + (-xz)$. Therefore, we need to show that $x(y + -z) = xy + (-xz)$. Since multiplication distributes over addition, $x(y + -z) = xy + x(-z)$. All that's left to show is that $-xz = x(-z)$.

To show that the negation of xz is equal to $x(-z)$, it's enough to show that $xz + x(-z) = 0$, but $z + (-z) = 0$, and multiplying that by x and applying distributivity it follows that $xz + z(-z) = 0$. Q.E.D.

21. Prove that 0 times any element in a field is 0: $0x = 0$.

Proof. Since $0 + 0 = 0$, therefore $0x + 0x = 0x$ by distributivity. Subtracting $0x$ from each side, $0x = 0$. Q.E.D.

That proof could be given more details. Subtracting $0x$ really means adding $-0x$. So from $0x + 0x = 0x$, the next equation is $(0x + 0x) + (-0x) = 0x + (-0x)$. Then by associativity, $0x + (0x + (-0x)) = 0x + (-0x)$. Next, since $0x + (-0x) = 0$, we get $0x + 0 = 0$, then since 0 is the additive identity, therefore $0x = 0$.

To be absolutely complete it's necessary to put in all the steps and a justification for each step. As you go along, you can skip some of that detail if you know how to supply it if asked. You'll get a good idea of what you can fill in as you gain experience in developing and writing proofs.

22. Prove the following properties concerning multiplication by negatives: $(-1)x = -x$, $-(-x) = x$, $(-x)y = -(xy) = x(-y)$, and $(-x)(-y) = xy$.

Proof. To show $(-1)x = -x$. That says that -1 times x is the negation of x. To prove that, it's enough to prove that the sum of $(-1)x$ and x is 0. The equation $(-1)x + x = 0$ follows from $(-1)x + 1x = 0$, and that, by distributivity follows from $((-1) + 1)x = 0$. That itself, by exercise 21, follows from $(-1) + 1 = 0$, which is the definition of -1. Q.E.D.

Proof. To show $-(-x) = x$. To show the negation of $-x$ is x, it's enough to show that $(-x) + x = 0$, but that's the definition of $-x$. Q.E.D.

Proof. To show $(-x)y = -(xy) = x(-y)$. To show that $(-x)y$ is the negation of xy, it's enough to show that $(-x)y + xy = 0$. But that follows from $(-x) + x = 0$ by multiplying by y, and applying distributivity and exercise 21.

The other equation is similar, or you could note that it follows from the first equation by commutativity. Q.E.D.

Proof. To show $(-x)(-y) = xy$. From the preceding part $(-x)(-y) = -x(-y) = -(-xy)$ which equals xy by the second part of this exercise. Q.E.D.

23. Prove the following properties concerning reciprocals: $(x^{-1})^{-1} = x$, and $(xy)^{-1} = x^{-1}y^{-1}$.

The proofs are identical to some of those in the preceding exercise except everything is multiplicative instead of additive.

24. Prove that $\dfrac{x}{y} = \dfrac{w}{z}$ if and only if $xz = yw$.

It's assumed here that y and z are not 0 in order for them to appear in the denominators.

Use the definition of division, $\dfrac{x}{y} = x(y^{-1})$, and then use properties of multiplication. $\dfrac{x}{y} = \dfrac{w}{z}$ iff $x(y^{-1}) = w(z^{-1})$. Multiply by yz to get $x(y^{-1})yz = w(z^{-1})yz$. Replace $y^{-1}y$ by 1 and $z^{-1}z$ by 1 (and use commutativity to conclude $xz = yw$¿

For the reverse direction, multiply by $y^{-1}z^{-1}$ instead of yz.

25. Prove the following properties concerning division: $\dfrac{x}{y} \pm \dfrac{w}{z} = \dfrac{xz \pm yw}{yz}$, $\dfrac{x}{y}\dfrac{w}{z} = \dfrac{xw}{yz}$, and $\dfrac{x}{y}\Big/\dfrac{w}{z} = \dfrac{xz}{yw}$.

Here's an equational proof of $\dfrac{x}{y} + \dfrac{w}{z} = \dfrac{xz + yw}{yz}$. An equational proof is one long continued equation that starts with the term on the left side and ends with the term on the right side.

$$\begin{aligned} \frac{x}{y} + \frac{w}{z} &= xy^{-1} + wz^{-1} \\ &= xy^{-1}zz^{-1} + wz^{-1}yy^{-1} \\ &= (xz + yw)y^{-1}z^{-1} = \frac{xz + yw}{yz} \end{aligned}$$

In an equational proof, it should be obvious what the justification for each equality is. If it's not then supply the justification. Associativity and commutativity aren't usually mentioned because associativity is implicitly used every time a ternary sum or difference is used, and commutativity is easily recognized as the terms get exchanges. The above equational proof used both. Distributivity is also easily recognized as well as basic properties of 0, 1, negations, reciprocals, and definitions of subtraction and division.

26. Prove that if $xy = 0$, then either $x = 0$ or $y = 0$.

Proof. If x is not 0, then it has an inverse x^{-1}. Multiply the equation $xy = 0$ by x^{-1} to get $y = 0$. This if x is not 0, then y is 0. Either $x = 0$ or $y = 0$. Q.E.D.

Math 225 Home Page at
`http://aleph0.clarku.edu/~djoyce/ma225/`